SUPERSINGULAR HYPERELLIPTIC CURVE OF GENUS 2 OVER FINITE FIELDS

Y. CHOIE, E. JEONG, AND E. LEE

ABSTRACT. In this paper we describe an elementary criterion to determine supersingular hyperelliptic curve of genus 2, using only the given Weierstrass equation. Furthermore, we show that the discrete logarithm problem defined on any supersingular abelian variety of dimension 2 over $\mathbb{F}_p, p > 16$, can be embedded to that over the extension field $\mathbb{F}_{p^k}$, with $k \leq 6$. This implies that supersingular hyperelliptic curves are cryptographically weaker than the general case due to the Frey-Rück attack. A family of the hyperelliptic curve $H/\mathbb{F}_p$ of the type $v^2 = u^5 + a$ and $v^2 = u^5 + au$ have been studied and further examples are listed.

1. Introduction

It is known that using the Tate pairing, the discrete logarithm problem on the divisor class group $J_C(\mathbb{F}_q)$ of a curve C over the finite field $\mathbb{F}_q$ can be reduced to that over $\mathbb{F}_{q^k}$ of some extension of the base field. When k is small one can solve the discrete logarithm problem using an index calculus method over the finite field and this is called the *Frey-Rück attack*[5]. Menezes, Okamoto and Vanstone showed that for the supersingular elliptic curves the value k above is at most 6 and, therefore, the good upper bound of the complexity of the attack in the supersingular elliptic curve could be provided[12] . It follows that the supersingular elliptic curve should be considered insecure for cryptosystem. On the contrary, there are many constructive applications of supersingular elliptic curves(supersingular curves in general[6])(see, for instance,

Keynote: Supersingular Hyperelliptic curve, Cryptography, Discrete logarithm.

1991 Mathematics Subject Classification: Primary 11G20, 11T71 14G50 Secondary 11T55 14G10 .

This work was partially supported by MSRC.

[10]). Recently, Boneh and Franklin[3] suggested to use of supersingular elliptic curves(supersingular curves in general[6]) to generate an indentity based encryption scheme.

Since Koblitz suggested using the hyperelliptic curve H as a good source of public key cryptosystem, many interesting results have been explored toward hyperelliptic cryptosystem. When the genus g of the curve is large, there is a subexponential algorithm due to Adleman, DeMarrais and Huang[1] for the discrete logarithm problem in $J_H(\mathbb{F}_q)$. Also, when the genus g of a curve is small but $g \geq 4$, Gaudry's algorithm is faster than Pollard's rho algorithm[9]. Consequently, the hyperelliptic curves of genus $2, 3$ can be very attractive for the cryptographic purpose.

However, one needs to check if a given hyperelliptic curve of genus 2 and 3 is secure under the Frey-R*ü*ck attack. When using the Tate pairing, the upper bound of the extension degree k is determined as followings; let ℓ be the largest prime dividing $|J_H(\mathbb{F}_q)|$. Then k is the smallest integer such that $\ell | q^k - 1$. So, it will be very useful to detect those cryptographically weak curves in advance. Galbraith[6] showed that for supersingular curves there is an upper bound, which depends only on genus, on the values of the extension degree k, and in particular, it turns out that k can be at most 12 for the supersingular curve of genus 2. To determine, with known criterions, if the given curves are supersingular (see, for instance, [6, 18]), one needs to compute the number of rational points $|H(\mathbb{F}_{q^i})|$ of H, for all $i,\ 1 \leq i \leq g$, or, to know the characteristic polynomial of H. Therefore, when the characteristic p of the base field of the curve is large, this procedure is not really practical.

In this paper, we show that we can check, directly using the defining equation, if a given hyperelliptic curve H of genus 2 over $\mathbb{F}_q$, with $q = p^n, p > 2$, is supersingular. The criterion described in this paper can be used as a theoretical method to show whether curves are supersingular. In particular, we derive that any supersingular hyperelliptic curve H of genus 2 over $\mathbb{F}_p, p > 16$ can be embedded to the extension field $\mathbb{F}_{p^k}$, with $k \leq 6$. This implies that supersingular hyperelliptic curves are cryptographically weaker than the general case due to the Frey-R*ü*ck attack. Finally, as an example, using the above criterion, we determine all primes p where the hyperelliptic curves $H/\mathbb{F}_p$ of the type $v^2 = u^5 + a$ are supersingular. The orders of Jacobians of the above curves are determined and, therefore, the upper bounds of k are all determined. Further examples of the curve $H/\mathbb{F}_p$ with the defining equation, $v^2 = u^5 + au$ are discussed.

This paper is organized as follows. In Section 2 we introduce the usual notations and recall basic definitions of the Hyperelliptic curve of genus 2. In Section 3 we derive the main criterion how to determine if the given hyperelliptic curve of genus 2 is supersingular, directly using the defining equation and the proofs of the main theorem and lemmata will be postponed until the last Section 8. Section 4 states a complete characterization of supersingular abelian varieties of dimension 2 over the prime field $\mathbb{F}_p$. In Section 5, as an application of the main criterion, we characterize all the hyperelliptic curves $H/\mathbb{F}_p$ with defining equation of the type $v^2 = u^5 + a$. We also discuss examples of the type, $v^2 = u^5 + au, a \in \mathbb{F}_p^*$, in Section 6 and further examples are listed in Section 7.

2. **Hyperelliptic Curves over Finite Fields**

We recall the useful result related to the order of hyperelliptic curve over finite field. We follow definitions given in [**?**].

Let $\mathbb{F}_q$ be a field with $q = p^n$ elements of characteristic p and $\overline{\mathbb{F}_q}$ be its algebraic closure of $\mathbb{F}_q$. For a simplicity, take $p > 2$ throughout this paper.

Definition 2.1. A *hyperelliptic curve* H of genus g over $\mathbb{F}_q$ is a projective non-singular irreducible curve of genus g defined over $\mathbb{F}_q$ with a map $H \to \mathbb{P}^1$ of degree two. Here $\mathbb{P}^s$ denotes the s-dimensional projective space over $\mathbb{F}_q$. Moreover, we assume that H has an $\mathbb{F}_q$-rational point P such that the $\mathbb{F}_q$-rational function field of H has a nonconstant function whose only pole is a double one at P; such a point P is called a *Weierstrass point.*

Definition 2.2. A Weierstrass equation H of genus g over $\mathbb{F}_q, q = p^n$ is an equation of the form

$$H/\mathbb{F}_q \,:\, v^2 = f(u), f \in \mathbb{F}_q[u], \quad \deg f = 2g + 1,\ f \text{ monic}$$

with no singular affine points.

Remark 2.3. It is known that the curve H has a unique point $\mathcal{O}$ at infinity; namely $\mathcal{O} = [0, 0, 1]$ in the homogeneous coordinates $u = \frac{x_1}{x_0}, v = \frac{x_2}{x_0}$. Moreover, $\mathcal{O}$ is a singular point of multiplicity $2g - 1$ and the line at infinity $x_0 = 0$ is tangent to the curve at this point.

The following definition gives the notion of supersingularity of the curve, which is an analogue of that for an elliptic curve(see [6][18]).

Definition 2.4. An abelian variety A of dimension 2 over $\mathbb{F}_q$ is called *supersingular* if A is isogenus (over $\overline{\mathbb{F}_q}$) to a product of g supersingular elliptic curves. A curve C over $\mathbb{F}_q$ is called *supersingular* if the Jacobian $J_C(\mathbb{F}_q)$ of C is supersingular.

3. **Main Theorem**

There are criterions to check whether or not abelian variety A is supersingular, once its characteristic polynomial is computed. This means that the number of rational points $|A(\mathbb{F}_{q^i})|$ of A for all $i, 1 \leq i \leq g$ of the given abelian variety A needs to be computed. However, if the defining field $\mathbb{F}_q$ has a large prime characteristic p, the above criterions are not efficient to test supersingularity.

However, for a hyperelliptic curve of genus 2, there is a criterion to check if the given curve is supersingular, directly using the defining Weierstrass equation. In particular, when a curve is defined over the large prime field, the introduced method can give an effective test.

Let H be a hyperelliptic curve of genus 2 over a finite field $K = \mathbb{F}_q$ with $q = p^n,\ p > 2$, given by the following Weierstrass equation;

$$H/K : v^2 = f(u), f(u) \in K[u], \text{ monic with } \deg f(u) = 5.$$

We now state one of the main result.

Theorem 3.1. *Let H be the hyperelliptic curve of genus 2 over $K = \mathbb{F}_q$. Let A_d is the coefficient of the term x^{d-1} in $f(x)^{\frac{p-1}{2}}$. Then the following is true.*

(1) If H is supersingular, then

$$A_p \cdot A_{2p-1} = A_{p-1} \cdot A_{2p}. \tag{3.1}$$

(2) In particular, when H is defined over the prime field $\mathbb{F}_p$, i.e. $q = p$,

H is supersingular iff

$$A_p \cdot A_{2p-1} = A_{p-1} \cdot A_{2p} \;\; \textit{and} \;\; A_p + A_{2p-1} = 0. \tag{3.2}$$

Remark 3.2. Theorem3.1 can be practical to determine if given hyperelliptic curve H of genus 2 is supersingular when the defining field of H is a prime field $\mathbb{F}_p$, p large. We will discuss examples in section 5 and 6.

Before we prove the above theorem, we recall the following known criterion for supersingularity[6, 18].

Theorem 3.3. *Let A be an abelian variety of dimension 2 over $\mathbb{F}_q, q = p^n$. Assume*

$$P(x) = x^4 + a_1x^3 + a_2x^2 + qa_1x + q^2$$

is the characteristic polynomial of the Frobenius endomorphism on A. Then

(1) A is supersingular iff $p^{\lceil \frac{rn}{2} \rceil} | a_r$, for all $r = 1, 2$.

(2) Let $M_i = |A(\mathbb{F}_{q^i})|$ be the number of rational points of the abelian variety of dimension 2 over $\mathbb{F}_{q^i}, i = 1, 2$. Then the following holds;

$$a_1 = M_1 - 1 - q, a_2 = (M_2 - 1 - q^2 + a_1^2)/2.$$

Proof (1) See Theorem6.1 in [6].

(2) See page 147 of [11]. □

To prove Theorem3.1, we need the following recursive formulas among the coefficients of $f(u)^{\frac{q-1}{2}}$.

Lemma 3.4. *Let A_{dq+e} be the coefficient of x^{dq+e-1} in $f(u)^{\frac{q-1}{2}}$. For $n \geq 2$, the following relations hold;*

$$\begin{array}{llll}
(i) & A_{p^n} & = & A_p^{p^{n-1}} \cdot A_{p^{n-1}} + A_{p-1}^{p^{n-1}} \cdot A_{2p^{n-1}} \\
(ii) & A_{p^n-1} & = & A_p^{p^{n-1}} \cdot A_{p^{n-1}-1} + A_{p-1}^{p^{n-1}} \cdot A_{2p^{n-1}-1} \\
(iii) & A_{2p^n} & = & A_{2p}^{p^{n-1}} \cdot A_{p^{n-1}} + A_{2p-1}^{p^{n-1}} \cdot A_{2p^{n-1}} \\
(iv) & A_{2p^n-1} & = & A_{2p}^{p^{n-1}} \cdot A_{p^{n-1}-1} + A_{2p-1}^{p^{n-1}} \cdot A_{2p^{n-1}-1}
\end{array}$$

The following result states that the modular condition of the coefficients of the characteristic polynomial can be relaxed.

Lemma 3.5. *Suppose A is an abelian variety of dimension 2 over $\mathbb{F}_q$. Let*

$$P(x) = x^4 + a_1x^3 + a_2x^2 + qa_1x + q^2$$

be the characteristic polynomial of the Frobenius endomorphism on A. Then, for $r = 1, 2$,

$$a_r \equiv 0 \pmod p \quad \textit{iff} \quad p^{\lceil \frac{rn}{2} \rceil} | a_r. \tag{3.3}$$

Remark 3.6. Lemma3.5 was derived in [18] from the characterization of the simple abelian varieties over $\mathbb{F}_q$. In Section 6, we give an alternative proof of the above lemma using algebraic property.

4. Supersingular abelian variety of dimension 2 over $\mathbb{F}_p$

In this section, we focus more on the supersingular abelian varieties A over $\mathbb{F}_p$. Furthermore, an improved upper bound of k, where k is the smallest integer such that $\ell | p^{nk} - 1$, is derived in this case. Here ℓ is the exponent of $|A(\mathbb{F}_{p^n})|$.

Proposition 4.1. *Let A be any supersingular abelian variety of dimension 2 with genus 2 over $\mathbb{F}_p$, with a prime $p > 16$. Then there exists an integer k bounded by 6 such that, for every integer, $n \geq 1$, the exponent(the largest prime factor) of $|A(\mathbb{F}_{p^n})|$ divides $p^{nk} - 1$. Moreover, if $n \equiv 0 \pmod 2$ then this bound can be smaller, i.e. $k \leq 3$.*

Remark 4.2. (1) In fact, the order $|A(\mathbb{F}_{p^n})|$ is explicitly computed, for each n, when it exists.

(2) Galbraith[6] showed that the above embedding extension k is bounded by 12 for a supersingular abelian variety A of dimension 2 over the finite field $\mathbb{F}_q$. Proposition4.1 gives a better upper bound of k when the defining field is prime field.

(3) Furthermore, it is known that there exists k such that , for all $n \geq 1$, the exponent of $|A(\mathbb{F}_{p^n})|$ divides $p^{nk} - 1$. Although this was proved by Galbraith(see Theorem7 in [6]), we will give another elementary proof in this case.

5. Hyperelliptic curves of the type $v^2 = u^5 + a$ over $\mathbb{F}_p$

In this section we study a family of hyperelliptic curves of the form $v^2 = u^5 + a$ over $\mathbb{F}_p$ and determine all the primes p when it is supersingular as well as its Jacobian group structure[18] . Furthermore, we also get the upper bound of k.

Example 5.1. Consider the following hyperelliptic curve of genus 2;

$$H/\mathbb{F}_p : v^2 = u^5 + a, a \in \mathbb{F}_p^*.$$

(1) H is supersingular $\Leftrightarrow p \not\equiv 1 \pmod 5$.

(2) When $p \equiv 2, 3 \pmod 5$, the characteristic polynomial of H is $P(x) = x^4 + p^2$ and $|J_H(\mathbb{F}_p)| = 1 + p^2$. So, the smallest integer k such that the exponent ℓ of $|J_H(\mathbb{F}_{p^n})|$ divides $p^{nk} - 1$ is bounded by 4 for all $n \geq 1$.
Furthermore, $J(\mathbb{F}_p) \simeq \mathbb{Z}/(p^2 + 1)\mathbb{Z}$

(3) When $p \equiv 4 \pmod 5$, the characteristic polynomial of H is $P(x) = x^4 + 2px^2 + p^2$ and $|J_H(\mathbb{F}_p)| = p^2 + 2p + 1$. So, the smallest integer k such that the exponent ℓ of $|J_H(\mathbb{F}_{p^n})|$ which divides $p^{nk} - 1$, for all $n \geq 1$, is bounded by 2.
Furthermore, the group structure of Jacobians are given as follows[18];
If $p \not\equiv 3 \pmod{4,}$ then$J(\mathbb{F}_p) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$.
If $p \equiv 3 \pmod 4$, then $J(\mathbb{F}_p) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^a \times (\mathbb{Z}/\frac{p+1}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^b$, where $a + b = 2, a, b \in \mathbb{Z}, a, b \geq 0$.

Proof (1) We can check the following by direct computation;

$$A_p \neq 0 \Leftrightarrow p \equiv 1 \pmod 5, \quad A_{2p-1} \neq 0 \Leftrightarrow p \equiv 1 \pmod 5$$

$$A_{2p} \neq 0 \Leftrightarrow p \equiv 3 \pmod 5, \quad A_{p-1} \neq 0 \Leftrightarrow p \equiv 2 \pmod 5.$$

So, for any prime $p, A_{2p}A_{p-1} = 0$. By Theorem3.1, H is supersingular iff $A_pA_{2p-1} = 0, A_p + A_{2p-1} = 0$ and this is satisfied whenever $p \not\equiv 1 \pmod 5$.

(2) When $p \equiv 2, 3 \pmod 5$, gcd $(p - 1, 5) = 1$, gcd $(p^2 - 1, 5) = 1$. So,

$$\{x^5 + a | x \in \mathbb{F}_p\} = \mathbb{F}_p, \quad \{x^5 + a | x \in \mathbb{F}_{p^2}\} = \mathbb{F}_{p^2}.$$

$M_1 = 1 + p + \sum_{x \in \mathbb{F}_p} \chi(x^5 + a) = 1 + p + \sum_{x \in \mathbb{F}_p} \chi(x) = 1 + p.$
Similarly, $M_2 = 1 + p^2$. Therefore, the characteristic polynomial of H is $P(x) = x^4 + p^2$ and $|J_H(\mathbb{F}_p)| = 1 + p^2$.

(3) Let $P(x) = x^4 + a_1x^3 + a_2x^2 + a_1px + p^2$ be a characteristic polynomial. When $p \equiv 4 \pmod 5$, we know $a_1 = 0$ since H is supersingular by (1) and there are no prime $p < 16$ when $p \equiv 4 \pmod 5$. To compute the number of rational points M_2, we can write $M_2 = 1 + |R| + 2|Q|$, where $R = \{x \in \mathbb{F}_{p^2} | x^5 + a = 0\}$, $Q = \{x \in \mathbb{F}_{p^2} | x^5 + a$ is a non-zero quadratic residue in $\mathbb{F}_{p^2}\}$. Because $p^2 - 1$ is a multiple of 5 and $a \in \mathbb{F}_p^*$, R has 5 elements and $\mathbb{F}_{p^2}$ has a primitive 5-th root of unity, say ζ . If x_0 satisfies $x_0^5 + a = y_0^2$ for some $y_0 \in \mathbb{F}_{p^2}^*$, then $x_0\zeta^i$ does also for $0 \le i \le 4$. For fixed $y_0 \in \mathbb{F}_{p^2}^*$, the equation $x^5 + a = y_0^2$ doesn't have solutions or five solutions exept $y_0^2 = a$. In this case we have one solution $x = 0$. So $|Q| \equiv 1 \pmod 5$ and we have only one choice $a_2 = 2p$. Hence the characteristic polynomial of H is $P(x) = x^4 + 2px^2 + p^2$ and $|J_H(\mathbb{F}_p)| = p^2 + 2p + 1$. □

6. Hyperelliptic curves of the type $v^2 = u^5 + au$ over $\mathbb{F}_p$

In this section we study a family of hyperelliptic curves of the form $v^2 = u^5 + a$ over $\mathbb{F}_p$ and determine all the primes p when it is supersingular.

Example 6.1. Consider the following hyperelliptic curve of genus 2

$$H/\mathbb{F}_p : v^2 = u^5 + au,\ a \in \mathbb{F}_p^*.$$

Then

(1) H is supersingular iff $p \equiv 5, 7 \pmod 8$.
(2) The characteristic polynomial of H is one of the $P(x) = x^4 \pm 2px^2 + p^2$ and $|J_H(\mathbb{F}_p)| = p^2 \pm 2p + 1$.
(3) The group structures of Jacobians are given as follows[18];
  (i) If $p \equiv 5 \pmod 8$ and $P(x) = (x^2 + p)^2$, then $J(\mathbb{F}_p) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^2$
  (ii) If $p \equiv 7 \pmod 8$ and $P(x) = (x^2 - p)^2$, then $J(\mathbb{F}_p) \simeq (\mathbb{Z}/(p-1)\mathbb{Z})^2$
  (iii) If $p \equiv 5 \pmod 8$ and $P(x) = (x^2 - p)^2$, then $J(\mathbb{F}_p) \simeq (\mathbb{Z}/(p-1)\mathbb{Z})^a \times (\mathbb{Z}/\frac{p-1}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^b$, where $a + b = 2, a, b \in \mathbb{Z}, a, b \ge 0$.

(iv) If $p \equiv 7 \pmod 8$ and $P(x) = (x^2+p)^2$, then $J(\mathbb{F}_p) \simeq (\mathbb{Z}/(p+1)\mathbb{Z})^a \times (\mathbb{Z}/\frac{p+1}{2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})^b$, where $a+b=2, a,b \in \mathbb{Z}, a,b \geq 0$.

Proof (1) A direct computation shows that

$$A_p \neq 0 \Leftrightarrow p \equiv 1 \pmod 8, \quad A_{2p-1} \neq 0 \Leftrightarrow p \equiv 1 \pmod 8$$

$$A_{2p} \neq 0 \Leftrightarrow p \equiv 3 \pmod 8, \quad A_{p-1} \neq 0 \Leftrightarrow p \equiv 3 \pmod 8.$$

If $p \equiv 1 \pmod 8$, then $A_{2p} = A_{p-1} = 0$ but $A_p A_{2p-1} \neq 0$.
If $p \equiv 3 \pmod 8$, then $A_p = A_{2p-1} = 0$ but $A_{2p} A_{p-1} \neq 0$.
but if $p \equiv 5, 7 \pmod 8$, then $A_p = A_{2p-1} = A_{2p} = A_{p-1} = 0$. So, the result follows from Theorem3.1.

(2) Let $P(x) = x^4 + a_1 x^3 + a_2 x^2 + a_1 p x + p^2$ be a characteristic polynomial. Then, we get $a_1 = 0$ for $p = 5, 7, 13$ by a direct computation and for $p > 16$ by Hasse bound. By the same reason as the proof (3) in Example 5.1, we can write $M_2 = 1 + |R| + 2|Q|$, where $R = \{x \in \mathbb{F}_{p^2} | x^5 + ax = 0\}$, $Q = \{x \in \mathbb{F}_{p^2} | x^5 + ax$ is a non-zero quadratic residue in $\mathbb{F}_{p^2}\}$. Since $p^2 \equiv 1 \pmod 8$, $a \in \mathbb{F}_p^*$, R has 5 elements and $\mathbb{F}_{p^2}$ has a primitive 8th root of unity, say ζ. If $x_0 \in Q$, then $x_0 \zeta^{2i} \in Q$, for all $i, 0 \leq i \leq 3$. So $|Q|$ is a multiple of 4 and, by using this, we can get $a_2 = 2p$ or $a_2 = -2p$ since $p \equiv 5, 7 \pmod 8$. □

7. Further Examples

We list further examples of the various types of hyperelliptic curve of genus 2. In particular, for the small characteristic case we classify all the supersingular curves in terms of defining equations.

Example 7.1. Every supersingular hyperelliptic curve of genus 2 over $\mathbb{F}_3$ is isomorphic to the following form

$$H/\mathbb{F}_3 : v^2 = u^5 + bu^3 + e, e \neq 0$$

Proof Let $H : v^2 = u^5 + au^4 + bu^3 + cu^2 + du + e$ be a hyperelliptic curve of genus 2. Then $A_p = A_3 = c, A_{2p-1} = A_5 = a, A_{p-1} = A_2 = d, A_{2p} = A_6 = 1$. Theorem3.1 states that H is supersingular iff $a + c = 0, ac = d$. So all supersingular curves over $\mathbb{F}_3$ should be the following form

$$v^2 = u^5 + au^4 + bu^3 - au^2 - a^2 u + e$$

By changing variable $u + a \to u$, we get the result. $\square$

Example 7.2. Every supersingular hyperelliptic curve of genus 2 over $\mathbb{F}_5$ is isomorphic to the following forms

$$H/\mathbb{F}_5 : \begin{cases} v^2 = u^5 + du + e, d \neq 0 \\ v^2 = u^5 + au^4 + cu^2 + c^{-1}a^3u + 2(a + a^{-1}c^2), ac \neq 0 \end{cases}$$

Proof Let $H : v^2 = u^5 + au^4 + bu^3 + cu^2 + du + e$ be a defining equation of hyperelliptic curve of genus 2.
Then note $A_p = A_5 = c^2 + 2ae + 2bd$, $A_{2p-1} = A_9 = a^2 + 2b$, $A_{p-1} = A_4 = 2be + 2cd$, $A_{2p} = A_{10} = 2a$.
Theorem3.1 implies that H is supersingular iff $a^2 + 2b + c^2 + 2ae + 2bd = 0$ and $a^2b + b^2 + abe + acd = 1$.
(Case 1) If $a = 0$, then $b = c = 0$. So, H is $v^2 = u^5 + du + e$.
(Case 2) If $a \neq 0$, then $d = (b^2-ac)^{-1}(3a^2b+2bc^2-1), e = a^{-1}(2a^2-b+2c^2-bd)$.
Note that $b^2 \neq ac$. Replacing $u + a^{-1}b \to u$ we can get the desired form. $\square$

Example 7.3. Consider the following hyperelliptic curve of genus 2 over $\mathbb{F}_p$

$$H/\mathbb{F}_p : u^5 + bu^3 + du, bd \neq 0, p \equiv 3 \pmod 4$$

H is supersingular iff

$$\sum_{i=0}^{[\frac{p-3}{8}]} \begin{pmatrix} \frac{p-1}{2} \\ i \end{pmatrix} \begin{pmatrix} \frac{p-1}{2} - i \\ \frac{p-3}{4} - 2i \end{pmatrix} (\frac{d}{b^2})^i = 0$$

or

$$\sum_{i=\frac{p+1}{4}}^{[\frac{3p-1}{8}]} \begin{pmatrix} \frac{p-1}{2} \\ i \end{pmatrix} \begin{pmatrix} \frac{p-1}{2} - i \\ \frac{3p-1}{4} - 2i \end{pmatrix} (\frac{d}{b^2})^i = 0$$

Proof Note that if $p \equiv 3 \pmod 4$, then $A_p = A_{2p-1} = 0$. So, Theorem3.1 implies that it is enough to check that $A_{p-1}A_{2p} = 0$. A direct computation leads the equations in the statement. $\square$

8. **Proofs**

In this section, proofs of theorems and lemmata given in Section3 and 4 are derived.

Proof of Lemma3.4

Since $charK = p$ and we can write

$$f(x)^{\frac{p^n-1}{2}} = (f(x)^{\frac{p-1}{2}})^{p^{n-1}} \cdot f(x)^{\frac{p^{n-1}-1}{2}},$$

the coefficient of the term x^{dq+e-1} of the left side is derived from those of the term x^i and x^j in $f(x)^{\frac{p^n-1}{2}}$ has the index satisfying

$$dp^n + e - 1 = i \cdot p^{n-1} + j \tag{8.1}$$

for four cases of (d, e) where

$$0 \le i \le \frac{5(p-1)}{2},\ 0 \le j \le \frac{5(p^{n-1}-1)}{2}. \tag{8.2}$$

Since $p^{n-1} \ge 3$, we have

$$dp^n + e - i \cdot p^{n-1} = j + 1 \ge 1, \quad \text{and} \quad dp^n + e - 1 - i \cdot p^{n-1} = j \le \frac{5(p^{n-1}-1)}{2},$$

we get upper bounds and low bounds for i as follows;

(i) If $(d, e) = (1, 0)$, then

$$p^{n-1} \cdot (p - i) \ge 1 \quad \text{and} \quad p - \frac{5}{2} + \frac{3}{2} \cdot \frac{1}{p^{n-1}} \le i$$

and thus $p - 2 \le i \le p - 1$.

(ii) If $(d, e) = (1, -1)$, then

$$p^{n-1} \cdot (p - i) \ge 2 \quad \text{and} \quad p - \frac{5}{2} + \frac{1}{2} \cdot \frac{1}{p^{n-1}} \le i$$

and thus $p - 2 \le i \le p - 1$.

(iii) If $(d, e) = (2, 0)$, then

$$p^{n-1} \cdot (2p - i) \ge 1 \quad \text{and} \quad 2p - \frac{5}{2} + \frac{3}{2} \cdot \frac{1}{p^{n-1}} \le i$$

and thus $2p - 2 \le i \le 2p - 1$.

(iv) If $(d, e) = (2, -1)$, then

$$p^{n-1} \cdot (2p - i) - 1 \ge 1 \quad \text{and} \quad 2p - \frac{5}{2} + \frac{1}{2} \cdot \frac{1}{p^{n-1}} \le i$$

and thus $2p-2 \le i \le 2p-1$.

Finally, we get the desired i and j from (8.1).

$\square$

Proof of Lemma3.5
Since "if" statement is trivial, we claim "only if" part.
Let $\alpha_i, 1 \le i \le 4$, be the roots of $P(x)$ which are arranged in a way that $\alpha_1\alpha_3 = \alpha_2\alpha_4 = q$ holds (Theorem.V.1.15,p.166 in [17]). In case the splitting field K of $P(x)$ is different from $\mathbb{Q}(\alpha_1)$ or $\mathbb{Q}(\alpha_2)$, from elementary algebra we can choose a primitive element of the splitting field $K = \mathbb{Q}(\alpha_1, \alpha_2)$ as follows; take $\gamma = \alpha_1 + a\alpha_2$, where a satisfies

$$a \neq \frac{\alpha_i - \alpha_1}{\alpha_2 - \alpha_j} \text{ for } 1 \le i, j \le 4, j \neq 2 \text{ and } a \equiv 0 \pmod{p}.$$

So, $K = \mathbb{Q}(\gamma)$ or $K = \mathbb{Q}(\alpha_1) = \mathbb{Q}(\alpha_2)$.
Since $P(x) \equiv x^4 \pmod{p}$, the minimal polynomial $g(x)$ of K should satisfy $g(x) \equiv x^{[K:\mathbb{Q}]} \pmod{p}$ if $K = \mathbb{Q}(\alpha_1)$. If $K = \mathbb{Q}(\gamma)$, then consider a monic polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(\gamma) = 0$ constructed as the following way; consider a matrix $M = (c_{kl})_{0 \le k,l < 16}$ whose entries are determined by the representation of each $\gamma\alpha_1^i\alpha_2^j, k = i+j$, by $\alpha_1^i\alpha_2^j, 0 \le l = i+j < 16$, where $0 \le i, j < 4$. Note that $f(x) = |xI - M|$ is a monic integral polynomial with the coefficients as combination of $a, q, q^2, a_1, a_1q, a_2$ and $f(\gamma) = 0$. This implies that $f(x) \equiv x^{16} \pmod{p}$ and, thus, the minimal polynomial $g(x)$ of γ should satisfy $g(x) \equiv x^{[K:\mathbb{Q}]} \pmod{p}$. If $\mathbb{Z}[\gamma]$ is p-maximal,i.e., $[O_K : \mathbb{Z}[\gamma]] \not\equiv 0 \pmod{p}$, O_K ring of integer of K, then $pO_K = \wp^{[K:\mathbb{Q}]}$ (Theorem 4.8.13, p.196, [4]). If $[O_K : \mathbb{Z}[\gamma]] \equiv 0 \pmod{p}$, (Proposition6.2.1 and 6.2.3, p.307 in [4]) implies that $pO_K = \wp$. Here, $\wp$ is a prime ideal in O_K dividing p. So, we showed that p is totally ramified or remains as a prime in K.
Now, let $P(x) = (x^2 - t_1x + q)(x^2 - t_2x + q)$ where $t_1 = \alpha_1 + \alpha_3, t_2 = \alpha_2 + \alpha_4 \in O_K$. Since $-a_1 = t_1 + t_2 \in pO_K \subset \wp$ and $a_2 = 2q + t_1t_2 \in pO_K \subset \wp$, t_1 and t_2 are in $\wp$ and thus all $\alpha_i \in \wp$. This implies that

$$\mathrm{ord}_\wp(\alpha_1) = \mathrm{ord}_\wp(\alpha_2) = \mathrm{ord}_\wp(\alpha_3) = \mathrm{ord}_\wp(\alpha_4)$$

which follows from the fact that $\alpha_j = \sigma(\alpha_i)$ for some $\sigma \in Aut(K)$ and $\sigma(\wp) = \wp$. Let $e = e(\wp \mid p)$ be the ramification index of p in O_K. Since

$$e \operatorname{ord}_p(q) = \operatorname{ord}_\wp(q) = \operatorname{ord}_\wp(\alpha_1) + \operatorname{ord}_\wp(\alpha_3) = \operatorname{ord}_\wp(\alpha_2) + \operatorname{ord}_\wp(\alpha_4),$$

we get, for all $i, 1 \leq i \leq 4$, $\operatorname{ord}_\wp(\alpha_i) = \frac{e}{2} \operatorname{ord}_p(q)$. Hence, the "only if" statement immediately follows from

$$\operatorname{ord}_p(a_1) \geq \tfrac{1}{e} \operatorname{ord}_\wp(\alpha_i) = \tfrac{1}{2} \operatorname{ord}_p(q)$$

and

$$\begin{aligned} \operatorname{ord}_p(a_2) = \operatorname{ord}_p(2q + t_1 t_2) &\geq \tfrac{1}{e} \min(\operatorname{ord}_\wp(q), \operatorname{ord}_\wp(t_1) + \operatorname{ord}_\wp(t_2)) \\ &= \tfrac{1}{e} \operatorname{ord}_\wp(q) = \operatorname{ord}_p(q). \end{aligned}$$

This proves Lemma. $\square$

Proof of Theorem3.1

First, note that

$$M_1 := |H(\mathbb{F}_q)| = 1 + q + \sum_{x \in \mathbb{F}_q} f(x)^{\frac{q-1}{2}} \text{ in } \mathbb{F}_q,$$

since $f(x)^{\frac{q-1}{2}} \in \{\pm 1\}$ in $\mathbb{F}_q^*$. From the cyclic nature of ${\mathbb{F}_q}^*$, the following is true

$$\sum_{x \in \mathbb{F}_q} x^i = \begin{cases} -1 \text{ if } (q-1)|i \\ 0 \text{ if } (q-1) \not| i \end{cases}$$

Since $f(x)$ has degree 5, by multiplying out $f(x)^{\frac{q-1}{2}}$ and sum over $x \in \mathbb{F}_q$, the only non-zero term comes from x^{q-1} and $x^{2(q-1)}$. Hence,

$$M_1 = 1 - A_q - A_{2q-1}.$$

Similarly, by letting

$$M_2 := |H(\mathbb{F}_{q^2})| = 1 + q^2 + \sum_{x \in \mathbb{F}_{q^2}} f(x)^{\frac{q^2-1}{2}} \text{ in } \mathbb{F}_{q^2},$$

we have

$$M_2 = 1 - A_{q^2} - A_{2q^2-1}.$$

On the other hand, since Theorem3.3$-$(2) implies that

$$a_1 = M_1 - 1 - q, a_2 = (M_2 - 1 - q^2 + a_1^2)/2$$

with the fact that a_1, a_2 are rational integers, we note that

$$H \text{ is supersingular} \Leftrightarrow a_1 \equiv 0 \pmod{p^{\lceil \frac{n}{2} \rceil}}, a_2 \equiv 0 \pmod{p^n}.$$

Since

$$A_q + A_{2q-1} = 0, A_{q^2} + A_{2q^2-1} = 0 \Leftrightarrow a_1 \equiv a_2 \equiv 0 \pmod p,$$

we can conclude that, from Lemma3.5,

$$H \text{ is supersingular} \Leftrightarrow A_q + A_{2q-1} = 0, A_{q^2} + A_{2q^2-1} = 0.$$

Now it remains to show that

$$A_q + A_{2q-1} = 0, A_{q^2} + A_{2q^2-1} = 0 \tag{8.3}$$

implies

$$A_p \cdot A_{2p-1} = A_{p-1} \cdot A_{2p}. \tag{8.4}$$

First, note that, from Lemma3.4,

$$\begin{aligned} A_{q^2} &= A_q^q \cdot A_q + A_{q-1}^q \cdot A_{2q} &&= -A_q \cdot A_{2q-1} + A_{q-1} \cdot A_{2q} \\ A_{2q^2-1} &= A_{2q}^q \cdot A_{q-1} + A_{2q-1}^q \cdot A_{2q-1} &&= A_{2q} \cdot A_{q-1} - A_{2q-1} \cdot A_q \end{aligned}$$

and, so, the equation (8.3) yields

$$A_{p^n} \cdot A_{2p^n-1} = A_{2p^n} \cdot A_{p^n-1}. \tag{8.5}$$

Again, with Lemma3.4, the equation (8.5) becomes

$$(A_p^{p^{n-1}} \cdot A_{2p-1}^{p^{n-1}} - A_{p-1}^{p^{n-1}} \cdot A_{2p}^{p^{n-1}}) \cdot (A_{p^{n-1}} \cdot A_{2p^{n-1}-1} - A_{p^{n-1}-1} \cdot A_{2p^{n-1}}) = 0.$$

If $(A_{p^{n-1}} \cdot A_{2p^{n-1}-1} - A_{p^{n-1}-1} \cdot A_{2p^{n-1}}) = 0$, then by induction on n the relation (8.4) can be derived. If not, i.e., $(A_p \cdot A_{2p-1})^{p^{n-1}} = (A_{p-1} \cdot A_{2p})^{p^{n-1}}$, then, again, the equation holds since p^{n-1} does not divide $p^n - 1$. This claims our main Theorem. $\square$

Proof of Proposition4.1

Let ℓ be the largest prime dividing $|A(\mathbb{F}_{p^n})| = J_n$ of A and let k be the smallest integer such that $\ell|(p^{nk} - 1)$.

Let $P(x) = x^4 + a_1x^3 + a_2x^2 + a_1px + p^2$ be the characteristic polynomial of pth Frobenius map. Since A is supersingular and $p > 16$, $a_1 = 0$ and $a_2 = 0, \pm p, \pm 2p$ by Lemma 3.5 and Hasse-Weil bound.

On the other hand, it is well known that $J_n = |A(\mathbb{F}_{p^n})| = |1 - \alpha^n|^2|1 - \beta^n|^2$, where α, β are roots of $P(x)$ and $|\ |$ is complex absolute. Let $t_n = \alpha^n + \bar{\alpha}^n$ and $s_n = \beta^n + \bar{\beta}^n$. Then $t_1 + s_1 = a_1 = 0$ and $2p + t_1s_1 = a_2$. This fact with a recursion formula $s_n = s_{n-1}s_1 - ps_{n-2}$ gives that $s_n = t_n$ if n is even, $s_n = -t_n$ otherwise. Hence it's enough to derive s_n or s_n^2 to determine $J_n = (1 - s_n + p^n)(1 - t_n + p^n)$ and k. Using the induction hypothesis, we can compute s_n according to a_2 as follows;

1. If a_2=0,then

$$\begin{cases} n \equiv 0 \pmod 8 & \Rightarrow & s_n = 2p^{n/2}, & J_n = (p^n - 2p^{n/2} + 1)^2, & \ell | p^n - 1 \\ n \equiv 4 \pmod 8 & \Rightarrow & s_n = -2p^{n/2}, & J_n = (p^n + 2p^{n/2} + 1)^2, & \ell | p^n - 1 \\ n \equiv 1,3 \pmod 4 & \Rightarrow & s_n^2 = 2p^n, & J_n = p^{2n} + 1, & \ell | p^{4n} - 1 \\ n \equiv 2 \pmod 4 & \Rightarrow & s_n = 0, & J_n = (p^n + 1)^2, & \ell | p^{2n} - 1 \end{cases}$$

2. If $a_2 = p$, then

$$\begin{cases} n \equiv 0 \pmod 6 & \Rightarrow & s_n = 2p^{n/2}, & J_n = (p^n - 2p^{n/2} + 1)^2, & \ell | p^n - 1 \\ n \equiv 1,5 \pmod 6 & \Rightarrow & s_n^2 = p^n, & J_n = p^{2n} + p^n + 1, & \ell | p^{3n} - 1 \\ n \equiv 2,4 \pmod 6 & \Rightarrow & s_n = -p^{n/2}, & J_n = (p^n + p^{n/2} + 1)^2, & \ell | p^{3n} - 1 \\ n \equiv 3 \pmod 6 & \Rightarrow & s_n^2 = 4p^n, & J_n = (p^n - 1)^2, & \ell | p^n - 1 \end{cases}$$

3. If $a_2 = -p$, then

$$\begin{cases} n \equiv 0 \pmod{12} & \Rightarrow & s_n = 2p^{n/2}, & J_n = (p^n - 2p^{n/2} + 1)^2, & \ell | p^n - 1 \\ n \equiv 1,5,7,11 \pmod{12} & \Rightarrow & s_n^2 = 3p^n, & J_n = p^{2n} - p^n + 1, & \ell | p^{6n} - 1 \\ n \equiv 2,10 \pmod{12} & \Rightarrow & s_n = p^{n/2}, & J_n = (p^n - p^{n/2} + 1)^2 & \ell | p^{3n} - 1 \\ n \equiv 3,9 \pmod{12} & \Rightarrow & s_n = 0, & J_n = (p^n + 1)^2, & \ell | p^{2n} - 1 \\ n \equiv 4,8 \pmod{12} & \Rightarrow & s_n = -p^{n/2}, & J_n = (p^n + p^{n/2} + 1)^2, & \ell | p^{3n} - 1 \\ n \equiv 6 \pmod{12} & \Rightarrow & s_n = -2p^{n/2}, & J_n = (p^n + 2p^{n/2} + 1)^2, & \ell | p^n - 1 \end{cases}$$

4. If $a_2 = 2p$, then

$$\begin{cases} n \equiv 0 \pmod 4 & \Rightarrow & s_n = 2p^{n/2}, & J_n = (p^n - 2p^{n/2} + 1)^2, & \ell | p^n - 1 \\ n \equiv 1,3 \pmod 4 & \Rightarrow & s_n = 0, & J_n = (p^n + 1)^2, & \ell | p^{2n} - 1 \\ n \equiv 2 \pmod 4 & \Rightarrow & s_n = -2p^{n/2}, & J_n = (p^n + 2p^{n/2} + 1)^2, & \ell | p^n - 1 \end{cases}$$

5. If $a_2 = -2p$, then

$$\begin{cases} n \equiv 0 \pmod 2 & \Rightarrow & s_n = 2p^{n/2}, & J_n = (p^n - 2p^{n/2} + 1)^2, & \ell | p^n - 1 \\ n \equiv 1 \pmod 2 & \Rightarrow & s_n^2 = 4p^n, & J_n = (p^n - 1)^2, & \ell | p^n - 1 \end{cases}$$

□

9. Conclusion

It will be very useful to detect those cryptographically weak curves such as supersingular curve in advance. Or, it will be also useful to find supersingular curve for a constructive application to generate an Identity based cryptosystem suggested by Boneh and Franklin[3] and generalized by Galbraith[6].

In this paper, we show how to determine if the given hyperelliptic curve of genus 2 over the finite field $\mathbb{F}_q$, q odd, is supersingular directly from the defining equation. In particular, when the defining field is the prime field $\mathbb{F}_p$, we show that any supersingular hyperelliptic curve H of genus 2 can be embedded to the extension field $\mathbb{F}_{p^k}$, with $k \leq 6$. Note that this bound is the same as that of supersingular elliptic curve case, which is called MOV-attack[12]. This implies that supersingular hyperelliptic curves are cryptographically weaker than the general case due to the Frey-Rück attack. Finally, as an example, using the above criterion, a family of the hyperelliptic curves $H/\mathbb{F}_p$ of the type $v^2 = u^5 + a$ and the type $v^2 = u^5 + au$ have been studied. Further examples are discussed to determine supersingularity from the equation for the small characteristic case. We expect that the similar criterions will be held for the case of genus 3 curves.

References

[1] L. Adleman, J. DeMarrais and M. Huang, A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields, Algorithmic Number Theory, LNCS 877 (1994), $28-40$, Springer-Verlag.

[2] I. Blake, Gadiel Seroussi and N. Smart, Elliptic Curves in Cryptography, London Math. Society, 265 (1999) Cambridge University Press.

[3] D. Boneh and M. Franklin, Identity-based Encryption from the Weil paring, Advances in Cryptology- CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, LNCS 2139, (2001), $21-229$, Springer-Verlag.

[4] H. Cohen, A Course in Computational Algebraic Number Theory, Springer-Verlag(1993).

[5] G. Frey and H-G. Rück, A remark concerning m-divisibility in the divisor class group of curves, Math.Comp. 62, No.206(1994), $865-874$.

[6] S. Galbraith, Supersingular curves in Cryptography, to appear in Asia Crypt(2001).

[7] S. Galbraith, F. Hess, N. P. Smart, Extending the GHS Weil descent attack, Preprint (2001).

[8] S. Galbraith, S. Paulus and N. Smart, Arithmetic on superelliptic curves , Math. Comp., Vol 71, pp 393-405, (2002).

[9] P. Gaudry, An algorithm solving the discrete log problem on hyperelliptic curves, Eurocrypt2000 Vol.1807, (2000), 19-34 LNCS 1807, Springer-Verlag.

[10] A. Joux, A one round protocol for tripartite Diffie-Hellman, ANTS-IV, LNCS 1838 (2000), 385-393, Springer-Verlag.

[11] N. Koblitz, Algebraic aspects of cryptography, Springer-Verlag (1998).

[12] A.J. Menezes, T. Okamoto and S.AQ. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Thans. Inf. Theory, 39 No5(1993), $1639 - 1646$.

[13] S. Siksek and N. Smart, A fast Diffie-Hellman protocol in genus 2, J. Cryptology, Vol 12, pp 67-73, (1999).

[14] J. Silverman, Arithmetic on Elliptic curves, Springer-Verlag (1986).

[15] N. Smart, On the performance of hyperelliptic cryptosystems, Proceedings EURO-CRYPT 99, Springer LNCS 1592, pp 165-175, (1999).

[16] N. Smart, A comparison of different finite fields for use in Elliptic Curve Cryptosystems, Computers and Mathematics with Applications, Vol 42, pp 91-100, (2001).

[17] H. Stichtenoth, Algebraic Function Fields and Codes, Springer Verlag (1993).

[18] C. Xing, On supersingular abelian varieties of dimension two over finite fields, Finite fields and their application $2, (1996), 407 - 421$.

Department of Mathematics, Pohang University of Science and Technology, Pohang, 790–784, Korea

E-mail address: `yjc@postech.ac.kr`

E-mail address: `ekjeong@euclid.postech.ac.kr`

E-mail address: `ejlee@postech.ac.kr`